REMARKS

Claims 2-21 are pending, of which claim 2 and 8 are independent method claims with corresponding independent computer program product claims 12 and 18. Claim 22 has been canceled without prejudice, and claims 2, 5, 8, 12, 15, and 18 have been amended as indicated above. Applicants note for the record that the subject matter of claim 22 has been incorporated into dependent claims 5 and 15, and therefore does not evince an intent to surrender any subject matter. As also indicated above, in the "Related Applications" section of this application, Applicants have corrected a typographical error with respect to the issue date of U.S. Patent No. 6,304,969, the parent of the present continuation.

The Office Action rejected each of the pending independent claims (2, 8, 12, and 18) under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,434,918 to Kung et al. ("*Kung*") in view of U.S. Patent No. 5,838,790 to McAuliffe et al. ("*McAuliffe*"). Each of the pending dependent claims was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* or over *Kung* in view of *McAuliffe* and U.S. Patent No. 6,161,185 to Guthrie et al. ("*Guthrie*").[1]

Applicants' invention, as claimed for example in independent claim 2, relates to a method of verifying that a server is authorized to provide resources to a client. In accordance with the method, a client generates a server authentication request to verify that the server is authorized to provide at least one resource to the client and transmits the request to the server. The method includes receiving an encrypted server authentication response from the server and decrypting the response without user interaction in order to prevent a user from colluding with an unauthorized server to circumvent server authentication. Unless the decrypted server authentication response indicates that the server is authorized to provide the at least one resource to the client, the method disables one or more client functions. Corresponding independent computer program product claim 12 recites similar limitations.

Applicants' invention, as claimed for example in independent claim 8, also relates to a method of verifying that a server is authorized to provide resources to a client. A client

[1] Applicants reserve the right to challenge *Kung, McAuliffe,* and *Guthrie* as a proper prior art references in the future. Accordingly, any statement in this response with respect to *Kung, McAuliffe,* and *Guthrie* is made merely assuming *arguendo* that *Kung, McAuliffe,* and *Guthrie* represent prior art and should not be interpreted as acquiescing the references asserted prior art status or teachings.

generates a server authentication request and transmits the request to the server. The client determines that no response to the server authentication request has been received after an allotted period of time, interprets no response as an indication that the server is not authorized to provide resources to the client, and disables one or more client functions. Corresponding independent computer program product claim 18 recites similar limitations.

Kung discloses mutual authentication of a user and a server on a network without exchanging a user's password in clear text. Col. 2, ll. 16-19. The client transmits a logon ID to the server. Col. 1, ll. 53-54. The server retrieves a user password corresponding to the logon ID and uses the password to encrypt a random number. Col. 1, ll. 54-60. To decrypt the random number and authenticate the server, the user enters the password at the client. Col. 1, ll. 60-65. This random number becomes the encryption and decryption key for communication between the client and server. Col. 1, ll. 66-67. The client sends a message encrypted with the random number to the server to authenticate the user. Col. 1, l. 67 – col. 2, l. 4.

McAuliffe discloses an advertisement system. In particular, *McAuliffe* uses a key-dependent one-way hash function to generate fingerprints of both advertisements downloaded to a user's computer and an advertisement statistics file (storing statistics as to which advertisements are shown to users, for how long, and at what times) which is periodically uploaded to a remote central computer. Col. 3, ll. 42-49. The fingerprints allow for detection of any tampering with, modification of, or replacement of the advertisements and statistics file. Abstract; col. 3, ll. 49-58. Remedial action, such as disabling client software, is taken only after multiple incidents of tampering are detected within a short time period for the same user. Col. 11, ll. 4-17.

In order to establish a *prima facie* case of obviousness, "the prior art reference (or references when combined) must teach or suggest <u>all</u> the claim limitations." MPEP § 2143 (emphasis added). During examination, the pending claims are given their broadest reasonable interpretation, i.e., they are interpreted as broadly as their terms reasonably allow, consistent with the specification. MPEP §§ 2111 & 2111.01.

Applicants respectfully submit, however, that for at least the reasons stated below *Kung* and *McAuliffe* fail to teach all the claim limitations of independent claims 2, 8, 12, and 18, as amended. For example, among other things, *Kung* and *McAuliffe* fail to teach or suggest decrypting the server authentication response without user interaction in order to prevent a user from colluding with an unauthorized server to circumvent server authentication, as recited in independent method claim 2 and corresponding independent computer program product claim 12. Rather, as indicated above, *Kung* discloses decrypting a random number received from a server with a password entered by a user at the client. Col. 1, ll. 60-65; Figure 2. (The Office Action relies solely on *Kung* for disclosing this limitation, without any reference to *McAuliffe*.)

In contrast to *Kung*, Applicants' Specification indicates that "[f]or a variety of reasons, suppliers or manufacturers of certain client systems may desire to allow only selected servers to provide network resources to their client systems." Specification, p. 3, ll. 15-17. Applicants note, however, that it is possible for a client system and the operator of an unauthorized server to collude in overriding conventional security systems based on user names, passwords, or other identifiers. *See* Specification, p. 3, l. 22 – p. 4, l. 12. *Kung's* user-entered password, therefore, merely represents one of the specific problems that Applicants' invention, as claimed for example in independent claims 2 and 12, attempts to solve. Accordingly, Applicants' respectfully submit that the rejection of independent claims 2 and 12 under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* has been overcome and should be withdrawn.

With respect to independent claims 8 and 18, the Office Action fails to address or even mention the limitation of "interpreting no response as an indication that the server is not authorized to provide resources to the client." Office Action, pp. 5-6 (rejection of claims 8 and 18). Because the Office Action fails to show that *Kung* and *McAuliffe* teach or suggest all the claim limitations of independent claims 8 and 18, Applicants respectfully submit that the Office Action has failed to establish a *prima facie* case of obviousness for claims 8 and 18, and therefore, the rejection of claims 8 and 18 under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* is improper and should be withdrawn.

Furthermore, in rejecting independent claims 8 and 18, the Office Action asserts that "disabling client functions after a number of incidents of 'tampering' in a time period" at column 11, lines 9-12 of *McAuliffe* meets the limitation of "after an allotted period of time, determining that no response to the server authentication request has been received by the client." Office Action, p. 6 (rejection of claims 8 and 18). While this cited portion of *McAuliffe* discloses detecting multiple incidents of "tampering" within a short time period, no reference whatsoever is made to "determining that no response to the server authentication request has been received by the client after an allotted period of time." Although Applicants have not changed the scope of claims 8 and 18, Applicants nevertheless have amended claims 8 and 18, as indicated above, to place the phrase "determining that no response to the server authentication request has been received by the client" before the phrase "after an allotted period of time" to emphasize this point.

Accordingly, because *McAuliffe* fails to teach or suggest the limitation of "determining that no response to the server authentication request has been received by the client after an allotted period of time" Applicants respectfully submit that the Office Action has failed to establish a *prima facie* case of obviousness with respect to independent claims 8 and 18. Therefore, in addition to the reasons stated above, the rejection of claims 8 and 18 under 35 U.S.C. § 103(a) as being unpatentable over *Kung* in view of *McAuliffe* is improper and should be withdrawn.

Based on at least the foregoing reasons, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example in independent claims 2, 8, 12, and 18. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertion with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so.

For example, Applicants specifically note that contrary to the assertions made in the Office Action, *McAuliffe* fails to show periodically performing the limitations recited in dependent claims 5 and 10 while the server is authorized to provide at least one resource to the client. The issue here is not one of the client authenticating downloads from multiple servers, as asserted in the Office Action, but rather, authenticating the server again while the server is authorized to provide at least one resource to the client. Applicants have amended claims 5 and 10 to clarify this distinction.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 13th day of July, 2004.

Respectfully submitted,

Eric M Kamerath

RICK D. NYDEGGER
Registration No. 28,651
ERIC M. KAMERATH
Registration No. 46,081
Attorneys for Applicant
Customer No. 022913

EMK:kc
KC0000002780V001